

Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name: REGION 2 > VHA > VISN 16 > Central Arkansas HCS (Little Rock) > VistA - VMS System
OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-00

Each Veterans Affairs (VA) medical center uses VistA (formerly DHCP, Decentralized Hospital Computer Program), an integrated hospital information system. DHCP was an M-based internally developed portfolio and VistA encompasses DHCP and a variety of other clinical and administrative applications, some on single-use platforms. VistA is currently running on two core platforms, Microsoft Windows 2000 (W2K)/Cache and Virtual Memory System (VMS)/Cache. This facility operates the following: InterSystems Cache on VMS [VMS/Cache]. VistA is structured so that it can be customized in certain specialized areas and most local medical centers have taken advantage of this flexibility. Applications within VistA support a multitude of areas including medical imaging, supply management, decision support, medical research, and education. VHA began deploying DHCP in 1982 with a core set of applications. Today, VistA is one of the most comprehensive integrated health information systems in the United States. Since episode-of-care workload reporting was an initial motivation for corporate databases, most of VHA's corporate systems collect their information from VistA. Recent enhancements have clearly shifted the focus from workload to enabling the integration of clinical information from various disciplines, forming the basis for an automated and distributed health information system. The following is a list of user organizations and the type of data processing involved:

- Administrative Employees – personnel employee information, financial, budget, benefits, research awards and projects, publications, clinical programs, tuition reimbursement, travel activity
- Service and Package-level ADP Applications Coordinators (ADPACs) – user and menu management, package settings, output consolidation activities (FileMan reports and printing), and other application controls.
- System Administrators – hardware, operating system, Kernel, etc. (system management and maintenance)

Description of System/ Application/ Program:

Facility Name:	Central Arkansas Veterans Healthcare Systems		
Title:	Name:	Phone:	Email:
Privacy Officer:	Angela Waddles	501-257-2972	angela.waddles@va.gov
Information Security Officer:	Donna Haggard	501-257-2008	donna.haggard@va.gov
System Owner/ N16 Chief Information Officer:	Dale Nelson	479-444-5011	Riley.Nelson@va.gov

Information Owner:	Michael R. Winn	501-257-5400	michael.winn@va.gov
Facility Chief Information Officer:	James Hall	501-257-1531	james.hall@va.gov
Person Completing Document:	Billy Winkle	501-257-2084	billy.winkle@va.gov
Other Titles:	N/A		
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	8/11/2008		
Date Approval To Operate Expires:	08/2011		
What specific legal authorities authorize this program or system:	79VA19 -Title 38, United States Code, section 7301(a). 24VA19 -Title 38, United States Code, chapter 3, section 201(c)(1) and chapter 73, section 4115 99VA13 - 5 U.S.C. Chapters 11, 31, 33, 43, 61, 63, and 83; 76VA05 - 38 U.S.C. 501; 38 U.S.C. Chapter 74. 57VA135 - Title 10 United States Code (U.S.C.) chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55 121VA19 - Title 38, United States Code, Section 501 97VA105 - Section 527 of 38 U.S.C. and the Government Performance and Results Act of 1993, Public Law 103ndash;62		
What is the expected number of individuals that will have their PII stored in this system:	1,000,000		
Identify what stage the System / Application / Program is at:	Operations/Maintenance		
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	1987; approximately 23 years		
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes		
If No, please explain:			
Has a PIA been completed within the last three years?	Yes		
Date of Report (MM/YYYY):	2/15/2011		

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- ☒ Have any changes been made to the system since the last PIA?
- ☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☒ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☒ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☒ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

Yes

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

79VA19, 24VA19, 76VA05, 57VA135, 97VA105, 99VA13,

2. Name of the System of Records:

79VA19 Veterans Health Information Systems and Technology Architecture (VISTA) Records 24VA19 Patient Medical Records, 76VA05 General Personnel Records, 57VA135 Voluntary Service Records, 97VA105 Consolidated Data Information System, 99VA13 Automated Safety Incident Surveillance and Tracking System (ASISTS, 121VA19 National Patient Database.

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

<http://vaww.vhaco.va.gov/privacy/systemofrecords.htm>

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Yes

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Yes

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	VA File Database	For their treatment and care and the individuals will not disclose unless a consent is given.	Verbally	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	Individuals will not disclose unless a consent is given.	Written	Written
Service Information	VA File Database	For their treatment and care and the individuals will not disclose unless a consent is given.	Verbally	Written
Medical Information	VA File Database	For their treatment and care and the individuals will not disclose unless a consent is given.	Verbally	Written
Criminal Record Information				
Guardian Information	VA File Database	Individuals will not disclose unless a consent is given.	Verbally	Written
Education Information	VA File Database	Individuals will not disclose unless a consent is given.	Verbally	Written
Benefit Information	VA File Database	Individuals will not disclose unless a consent is given.	Verbally	Written

Other (Explain)	Verbal	Next-of-kin information and emergency contact information, such as name and telephone number, is collected from the veteran to use to contact other individuals in case of an emergency. In addition insurance and employment information is available on the veteran for use in billing for care.	Verbally	Written
-----------------	--------	--	----------	---------

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Medical Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Criminal Record Information	No			
Guardian Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Education Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA	Yes	Patient Records	Both PII & PHI	Any federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.
Other Veteran Organization	DAV/PAV	Yes	Patient Records	Both PII & PHI	Any federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.

Other Federal Government Agency			There is certain VHA VistA patient data that is shared with DoD through the Federal/Bidirectional Health information Exchange (FHIE/BHIE) Program under DUAs that have been in effect for several years. In addition, certain clinical information is being shared with CDC, also under an established DUA.	Any federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.
	DoD	Yes		Both PII & PHI
State Government Agency	ODVA	Yes	Patient Records	Both PII & PHI Any federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.
Local Government Agency	N/A			N/A

Research Entity	UALR	Yes	Reserch studies have access to patient information	Both PII & PHI	Any federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system? No

Please enter the name of the system:

Per responses in Tab 4, does the system gather information from an individual? No

If information is gathered from an individual, is the information provided:

- ☐ Through a Written Request
- ☐ Submitted in Person
- ☐ Online via Electronic Form

Is there a contingency plan in place to process information when the system is down? Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request? No

if yes, please check all that apply:

- ☐ Drug/Alcohol Counseling
- ☐ Mental Health
- ☐ HIV
- ☐ Research
- ☐ Sickle Cell
- ☐ Other (Please Explain)

Describe process for authorizing access to this data.

Answer: N/A

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.

How is data checked for completeness?

Answer: Data is reviewed by staff and confirmed and also compared to paper forms after data is entered electronically to ensure that all fields have been completed.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Administrative data is updated with each application for care. Each time a veteran is seen for an appointment, hospitalization, travel pay, etc. data is verified and updated at the time the patient presents for care or follow-up. For example, clinics verify address, next of kin and insurance information.

How is new data verified for relevance, authenticity and accuracy?

Answer: New data is compared with printed form or via patient verification. The veteran brings DD214 with them and it is verified. For example, the 1010 is printed and the veteran reviews and signs that the information is accurate. For example, the VISTA system is designed to identify inconsistencies in data that is reported and provides an exception list for several applications.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer: None

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Clinical information is retained for 75 years.

Explain why the information is needed for the indicated retention period?

Answer: Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.

What are the procedures for eliminating data at the end of the retention period?

Answer: Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b (Page 190). At the present time, VistA Imaging retains all images. We are performing a study to explore whether some images can be eliminated on an earlier schedule.

Where are these procedures documented?

Answer: VA Handbook 6300; Record Control Schedule 10-1

How are data retention procedures enforced?

Answer: The retention period is dependent on the type of data and the intended use, so retention period varies. VA Records Control Schedule 10-1 (page 8): Records Management Responsibilities: The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures. Field records officers are responsible for records management activities at their facilities. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with MARRA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures. Local policy Medical Center Memorandum 136-35 "Records Management Policy".

Has the retention schedule been approved by the National Archives and Records Administration (NARA)	Yes
---	-----

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?	No
--	----

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
If 'No' to any of the 3 questions above, please describe why: Answer:	
Is adequate physical security in place to protect against unauthorized access?	Yes
If 'No' please describe why: Answer:	
Explain how the project meets IT security requirements and procedures required by federal law. Answer: At the Department level the CIO's of Cyber & Information Security (OCIS) is responsible for the establishment of directives, policies, & procedures which are consistent with the provisions of General Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & other requirements that Vista-Legacy is and has been subject to. In addition, OCIA administers and manages Department-wide security solutions, such as anti-virus protection, authentication, vulnerability scanning & penetration testing, & intrusion detection systems, and incident response (800-61). At the Vista-Legacy project level - The Project Manager ensures that CIO-Provided security directives are integrated into the project's security plan & implemented by VA & Contractor staff throughout the project. Funding needs are dependent on IT security requirements identified in the system development life cycle (800-64)(u,e, rusj assessments (800-3-), certification and accreditation (800-37 and 500-53)), as well as identified security weaknesses that must be corrected.	
Explain what security risks were identified in the security assessment? (Check all that apply)	
<input checked="" type="checkbox"/> Air Conditioning Failure <input checked="" type="checkbox"/> Chemical/Biological Contamination <input checked="" type="checkbox"/> Blackmail <input checked="" type="checkbox"/> Bomb Threats <input checked="" type="checkbox"/> Burglary/Break In/Robbery <input type="checkbox"/> Cold/Frost/Snow	<input checked="" type="checkbox"/> Data Disclosure <input checked="" type="checkbox"/> Data Integrity Loss <input type="checkbox"/> Denial of Service Attacks <input checked="" type="checkbox"/> Earthquakes <input type="checkbox"/> Eavesdropping/Interception
	<input checked="" type="checkbox"/> Hardware Failure <input checked="" type="checkbox"/> Identity Theft <input checked="" type="checkbox"/> Malicious Code <input checked="" type="checkbox"/> Power Loss <input checked="" type="checkbox"/> Sabotage/Terrorism <input checked="" type="checkbox"/> Storms/Hurricanes

☐ Cold/Frost/Snow

☒ Communications Loss

☒ Computer Intrusion

☒ Computer Misuse

☒ Data Destruction

Answer: (Other Risks)

☒ Errors (Configuration and Data Entry)

☒ Fire (False Alarm, Major, and Minor)

☒ Flooding/Water Damage

☒ Fraud/Embezzlement

☒ Storms/Hurricanes

☒ Substance Abuse

☒ Theft of Assets

☒ Theft of Data

☒ Vandalism/Rioting

Explain what security controls are being used to mitigate these risks. (Check all that apply)

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Contingency Planning | <input checked="" type="checkbox"/> Personnel Security |
| <input checked="" type="checkbox"/> Audit and Accountability | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Incident Response | <input checked="" type="checkbox"/> Risk Management |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | | |
| <input checked="" type="checkbox"/> Configuration Management | <input checked="" type="checkbox"/> Media Protection | |

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: This facility conducts ongoing security control assessments to evaluate effectiveness of security controls and implements changes as necessary. All VHA employees are required to take VA Privacy Awareness training on a yearly basis to ensure all staff who handles PII/PHI is knowledgeable of VA policies and procedures and practice adequate data safety/security. Notices of Privacy Practice are made available to patients. Consents are obtained as directed by VA Directive.

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?
(Choose One)

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | The potential impact is high if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> | The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> | The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals. |

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?
(Choose One)

- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | The potential impact is high if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> | The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. |
| <input type="checkbox"/> | The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals. |

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon

- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | The potential impact is high if the loss of confidentiality could be expected to have a |
| <input type="checkbox"/> | The potential impact is moderate if the loss of confidentiality could be expected to have a |

the system or organization?

(Choose One)



The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.



The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system? N/A

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name	CARPI Gui
Description	Broker Application - automated med information exchange between VA and VBA.
Comments	This application allows VBA to view VHA data
Is PII collected by this minor application?	NO
Does this minor application store PII?	NO
If yes, where?	
Who has access to this data?	Approved VBA staff

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system? X=included

X ASISTS	X Beneficiary Travel	X Accounts Receivable	X Adverse Reaction Tracking
X Bed Control	X Care Management	X ADP Planning (PlanMan)	X Authorization/ Subscription
X CAPRI	X Care Tracker	X Bad Code Med Admin	X Auto Replenishment/ Ward Stock
X CMOP	X Clinical Reminders	X Clinical Case Registries	X Automated Info Collection Sys
X Dental	X CPT/ HCPCS Codes	X Clinical Procedures	X Automated Lab Instruments
X Dietetics	X DRG Grouper	X Consult/ Request Tracking	X Automated Med Info Exchange
X Fee Basis	X DSS Extracts	X Controlled Substances	X Capacity Management - RUM
X GRECC	X Education Tracking	X Credentials Tracking	X Capacity Management Tools
X HINQ	X Engineering	X Discharge Summary	X Clinical Info Resource Network
X IFCAP	X Event Capture	X Drug Accountability	X Clinical Monitoring System
X Imaging	X Extensible Editor	X EEO Complaint Tracking	X Enrollment Application System
X Kernal	X Health Summary	X Electronic Signature	X Equipment/ Turn-in Request
X Kids	X Incident Reporting	X Event Driven Reporting	X Gen. Med.Rec. - Generator
X Lab Service	X Intake/ Output	X External Peer Review	X Health Data and Informatics
X Letterman	X Integrated Billing	X Functional Independence	X ICR - Immunology Case Registry
X Library	X Lexicon Utility	X Gen. Med. Rec. - I/O	X Income Verification Match
X Mailman	X List Manager	X Gen. Med. Rec. - Vitals	X Incomplete Records Tracking
X Medicine	X Mental Health	X Generic Code Sheet	X Interim Mangement Support
X MICOM	X MyHealthEVet	X Health Level Seven	X Master Patient Index Vista
X NDBI	X National Drug File	X Hospital Based Home Care	X Missing Patient Reg (Original) A4EL
X NOIS	X Nursing Service	X Inpatient Medications	X Order Entry/ Results Reporting
X Oncology	X Occurrence Screen	X Integrated Patient Funds	X PCE Patient Care Encounter
X PAID	X Patch Module	X MCCR National Database	X Pharmacy Benefits Mangement
X Prosthetics	X Patient Feedback	X Minimal Patient Dataset	X Pharmacy Data Management
X QUASER	X Police & Security	X National Laboratory Test	X Pharmacy National Database
X RPC Broker	X Problem List	X Network Health Exchange	X Pharmacy Prescription Practice
X SAGG	X Progress Notes	X Outpatient Pharmacy	X Quality Assurance Integration
X Scheduling	X Record Tracking	X Patient Data Exchange	X Quality Improvement Checklist
X Social Work	X Registration	X Patient Representative	X Radiology/ Nuclear Medicine
X Surgery	X Run Time Library	X PCE Patient/ HIS Subset	X Release of Information - DSSI
X Toolkit	X Survey Generator	X Security Suite Utility Pack	X Remote Order/ Entry System
X Unwinder	X Utilization Review	X Shift Change Handoff Tool	X Utility Management Rollup
X VA Fileman	X Visit Tracking	X Spinal Cord Dysfunction	X CA Verified Components - DSSI
X VBECS	X VistALink Security	X Text Integration Utilities	X Vendor - Document Storage Sys
X VDEF	X Women's Health	X VHS & RA Tracking System	X Visual Impairment Service Team ANRV
X VistALink		X Voluntary Timekeeping	X Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system? N/A

1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS
Administrative Data Repository (ADR)	ePROMISE	Remedy Application
ADT	EYECAP	SAN
Agent Cashier	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System
Air Fortress	Financial Management System	Sentillion
Auto Instrument	Genesys	Stellant
Automated Access Request	Health Summary Contingency	Stentor
BDN 301	ICB	Tracking Continuing Education
Bed Board Management System	KOWA	Traumatic Brain Injury
Cardiff Teleform	Lynx Duress Alarm	VA Conference Room Registration VAMedSafe
Cardiology Systems (stand alone servers from the network)	MHTP	
CHECKPOINT	Microsoft Active Directory	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	Microsoft Exchange E-mail System	VHAHUNAPP1 VHAHUNFPC1
Combat Veteran Outreach Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	
CP&E	Mumps AudioFAX	VISTA RAD
Crystal Reports Enterprise	NOAHLINK	Whiteboard
Data Innovations	Omniceil	
DELIVEREX	Onvicord (VLOG)	
DICTATION-Power Scribe	Optifill	
DRM Plus	P2000 ROBOT	
	PACS database	

DSIT	Personal Computer Generated Letters
DSS Quadramed	PICIS OR
EDS Whiteboard (AVJED)	PIV Systems
EKG System	Q-Matic
Embedded Fragment Registry	QMSI Prescription Processing

Explain any minor application that are associated with your installation that does not appear in the list above.
Please provide name, brief description, and any comments you may wish to include.

Name Description Comments Is PII collected by this minor application? Does this minor application store PII? If yes, where? Who has access to this data?
--

Name Description Comments Is PII collected by this minor application? Does this minor application store PII? If yes, where? Who has access to this data?
--

Name Description Comments Is PII collected by this minor application? Does this minor application store PII? If yes, where? Who has access to this data?
--

(FY 2011) PIA: Final Signatures

Facility Name: REGION 2 > VHA > VISN 16 > Central Arkansas HCS (Little Rock) > VistA - VMS System

Title:	Name:	Phone:	Email:
--------	-------	--------	--------

Privacy Officer:	Angela Waddles	501-257-2972	angela.waddles@va.gov
------------------	----------------	--------------	-----------------------

Digital Signature Block

Information Security Officer:	Donna Haggard	501-257-2008	donna.haggard@va.gov
-------------------------------	---------------	--------------	----------------------

Digital Signature Block

System Owner/ N16 Chief Information
Officer:

Dale Nelson

479-444-5011

Riley.Nelson@va.gov

Digital Signature Block

Facility Chief Information Officer:

James Hall

501-257-1531

james.hall@va.gov

Digital Signature Block

Date of Report:

2/1/11

OMB Unique Project Identifier

029-00-01-11-01-1180-00

REGION 2 > VHA > VISN 16 >
Central Arkansas HCS (Little Rock)

Project Name

> VistA - VMS System

(FY 2011) PIA: Final Signatures

Facility Name:

REGION 2 > VHA > VISN 16 > Central Arkansas HCS (Little Rock) > Vista - VMS System

Title	Name	Phone	Email
-------	------	-------	-------

Privacy Officer:

Angela Waddles

501-257-2972

angela.waddles@va.gov

Angela
Waddles

Digitally signed by Angela Waddles
DN: cn=Angela Waddles, o=CAVHS,
ou=VHA,
email=Angela.Waddles@va.gov, c=US
Date: 2011.03.25 06:11:13 -05'00'

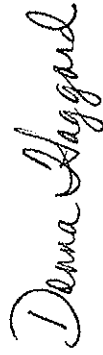
Digital Signature Block

Information Security Officer:

Donna Haggard

501-257-2008

donna.haggard@va.gov



Digitally signed by Donna Haggard
DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs,
ou=Internal Staff, 0.9.2342.19200300.100.1.1=donna.haggard@va.gov,
cn=Donna Haggard
Date: 2011.03.22 09:41:17 -05'00'

Digital Signature Block

System Owner/ N16 Chief Information

Officer:

Dale Nelson

479-444-5011

Riley.Nelson@va.gov



Digitally signed by Riley D. Nelson
DN: c=US, o=U.S. Government, ou=Department of
Veterans Affairs, ou=Internal Staff,
0.9.2342.19200300.100.1.1=Riley.Nelson@va.gov,
cn=Riley D. Nelson
Date: 2011.03.25 11:50:26 -05'00'

Digital Signature Block

Facility Chief Information Officer:

James Hall

501-257-1531

james.hall@va.gov



Digitally signed by James P Hall
Date: 2011.03.24 13:29:47 -05'00'

Digital Signature Block

Date of Report:

2/1/11

OMB Unique Project Identifier

029-00-01-11-01-1180-00

REGION 2 > VHA > VISN 16 >

Central Arkansas HCS (Little Rock)

> Vista - VMS System

Project Name